I hereby certify that this paper and/or fee is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 CFR §1.10 on the date indicated below and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature

DATE OF DEPOSIT: 01/14/02

EXPRESS MAIL LABEL NO.: EL 057 650 330 US

Inventor: David C. Challener

SUPER SECURE MIGRATABLE KEYS IN TCPA

FIELD OF THE INVENTION

The present invention relates to security in computer networks, and more particularly to protecting root keys in secure chips in the computer networks.

BACKGROUND OF THE INVENTION

Secure chips which follow the Trusted Computing Platform Alliance (TCPA) protocols are well known in the art. In this specification, a "secure chip" is a Trusted Platform Module (TPM). Typically, the TPM resides in a client computer system in a computer network. Among other functions, the TPM generates encryption keys in the form of public/private key pairs for the client to be used on the network. When the keys are not in use, they are stored outside of the TPM in a secure manner in a "daisy chain" fashion.

Figure 1 illustrates a conventional secure chip key chain. Assume that the secure chip 102 is a TPM. The TPM 102 has its own root key 104. The root key 104 is the mechanism which allows the storage of information by a TPM. The root key 104 comprises a public/private key pair for the TPM 102. The TPM 102 generates more keys, such as keys 106, for the network. At least one of these keys 106 is a migratable key. Each of these keys

106 comprise a public/private key pair. Each of these keys 106 is wrapped using the TPM's 102 public key. The TPM 102 can then generate children keys 108 and wrap them in the key's 106 public key. Other keys 110 may be generated and wrapped in the key's 108 public key. Thus, the chain comprises a child key 110, which is wrapped in the public key of the parent key 108; the parent key 108, which is wrapped in the public key of the grandparent key 106; and the grandparent key 106, which is wrapped in the public key of the TPM 102.

Keys can be of two types according to the TCPA specification: migratable and non-migratable. Migratable keys are particularly relevant to the present invention, and thus only they will be described here. The TCPA specification contains two commands for migrating keys from one TPM to another. The first is a simple re-wrap command, where a user's key is loaded into a TPM, unwrapped with its parent's key and then re-wrapped with another parent's key. This command can be used for migrating the user's key from one computer system to another during a computer upgrade. The second command is used for storing the user's key with a third party in case of hardware failure. For the second command, it is not known what the parent key of the replacement system will be during the storage, so a third party's public key is used for wrapping.

For the second command, if the third party's key may not be trusted, additional safeguards are provided. Before the key is wrapped, an optimal asymmetric encryption padding (OAEP) is applied and a random number, R, XOR'ed with the result before the final wrapping. This provides protection against the third party using his private key to unwrap the user's key. When the user's key is recalled from the third party, the user provides a public key (associated with the new TPM) to the third party in which to re-wrap the user's key, and then inserts the user's key wrapped with the new TPM's key along with R. The

TPM then unwraps the final wrapping, XOR's the result with R, reverses the OAEP and hence recovers the user's key. This key is then loaded into the new TPM. The new TPM re-wraps the key in a normal way, and the re-wrapped key is stored on the hard disk.

However, the private key of the root key 104 in the secure chip 102 may be read by peeling the TPM and examining the hardware. Once the root key 104 is obtained, it may be used to unwrap all of the grandparent keys 106 wrapped with the root key's public key. Having access to the grandparent keys 106 in turn allows the unwrapping of all of the parent keys 108, and then the child keys 110. This results in a serious security breach.

Accordingly, there exists a need for a method for providing improved security with a secure chip. The present invention addresses such a need.

SUMMARY OF THE INVENTION

A method for providing security with a secure chip, includes: creating a migratable keyblob using a first random number, where the migratable keyblob contains a key; wrapping the migratable keyblob with a public key of the key's parent key; encrypting the first random number with a pass phrase for a user of the key; storing the encrypted first random number; and migrating the migratable keyblob from the computer to itself. If the private key of the secure chip is stolen, the thief can only unwrap keys which are ancestors of the key in the migratable keyblob. To obtain the key in the migratable keyblob, the random number used to create it is required. However, the pass phrase of the user is required to decrypt it. This increases the security of the key stored in the migratable keyblob and its children keys.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 illustrates a conventional secure chip key chain.

Figure 2 illustrates a key chain created by a preferred embodiment of the method for improved security with a secure chip in accordance with the present invention.

Figure 3 is a flowchart illustrating a preferred embodiment of a method for improved security with a secure chip in accordance with the present invention.

Figure 4 is a flowchart illustrating in more detail the preferred embodiment of the method for improved security with a secure chip in accordance with the present invention.

Figure 5 is a flowchart illustrating how a key secured with the method in accordance with the present invention is obtained.

DETAILED DESCRIPTION

The present invention provides a method and system for providing improved security with a secure chip. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

To more particularly describe the features of the present invention, please refer to Figures 2 through 5 in conjunction with the discussion below.

Figure 2 illustrates a key chain created by a preferred embodiment of the method for

improved security with a secure chip in accordance with the present invention. In the preferred embodiment, the secure chip 102 stores one of the keys in the secure chip key chain in a migratable keyblob 202. For example, assume that a user of the parent key 108 desires improved security for the parent key 108 and its children keys 110. The parent key 108 is stored in a migratable keyblob 202 by scrambling the parent key 108 with an optimal asymmetric encryption padding (OAEP). The OAEP is well known in the art. The OAEP is then XOR'ed with a random number to create the migratable keyblob 202. The migratable keyblob 202 is then wrapped in the grandparent key's public key. With the present invention, the random number used to create the migratable keyblob 202 is generated by the secure chip's random number generator (not shown).

To use the parent key 108, the secure chip 102 unwraps the migratable keyblob 202 using its private key. To decrypt the migratable keyblob 202, the random number used to encrypt it must be available to the secure chip 102. With this random number, the secure chip 102 can unscramble the migratable keyblob 202 to obtain the parent key 108. However, the random number is typically many bits long, too long for the user to remember, and storing the random number on a disk with the secure chip 102 does not provide adequate security. To secure this random number, it too is encrypted using the pass phrase created by the user. The encrypted random number is then stored on the system. Thus, to obtain the parent key 108, the user's pass phrase is required. The pass phrase is used to decrypt the random number. This random number is then used by the secure chip 102 to obtain the parent key 108. Therefore, even if the secure chip's root key is discovered by peeling the chip 102, the parent key 108 stored in the migratable keyblob 202 is still not assessable without the pass phrase. If the migratable keyblob 202 cannot be decrypted, then the key's

children keys 110 are not assessable either. This increases the security of the secure chip in that portion of the secure chip's key chain.

Figure 3 is a flowchart illustrating a preferred embodiment of a method for improved security with a secure chip in accordance with the present invention. First, the secure chip 102 generates a first random number, via step 302. The first random number is used to create a migratable blob 202, via step 304. The migratable keyblob 202 contains a key, such as the parent key 108. The secure chip 102 then wraps the migratable keyblob 202 with the public key of the key's parent key, via step 306, which is the public key of the grandparent key 106. The secure chip 102 receives a pass phrase for the user of the key 108, via step 308. The secure chip 102 then generates a second random number based on the pass phrase, via step 310. A third random number is generated based on the second random number, via step 312. Next, a fourth random number is generated based on the first random number and the third random number, via step 314. This fourth random number is stored, via step 316. The migratable keyblob 202 is then migrated from the computer on which the secure chip 102 resides to itself, via step 318. In the preferred embodiment, the method is performed by a software residing on a disk in the computer on which the secure chip 102 also resides.

In this manner, if the root key 104 is somehow stolen, the thief can only unwrap keys in the key chain which are ancestors of the key stored in the migratable keyblob 202. To obtain the key in the migratable keyblob 202, the random number used to create the migratable keyblob 202 is required. This random number is stored encrypted such that the pass phrase of the user of the key is required to decrypt it. This increases the security of the key stored in the migratable keyblob 202. Since the key in the migratable keyblob 202 cannot be obtained, its children keys 110 also cannot be obtained. Thus, the method in

accordance with the present invention increases the security of keys in this portion of the key chain.

Figure 4 is a flowchart illustrating in more detail the preferred embodiment of the method for improved security with a secure chip in accordance with the present invention. Assume that the secure chip 102 is a Trusted Platform Module (TPM) using the Trusted Computing Platform Alliance (TCPA) protocol. First, a key, such as the parent key 108, is scrambled, via step 402. Next, the random number generator of the TPM 102 generates a first random number, via step 404. The first random number is then XOR'ed with the scrambled parent key 108 to create the migratable keyblob 202, via step 406. The TPM 102 wraps the migratable keyblob 202 with the public key of the parent key's parent key, i.e., the public key of the grandparent key 106, via step 408. Also, a pass phrase for a user of the parent key 108 is received, via step 410. A second random number is generated by hashing the user's pass phrase, via step 412. A third random is generated number by applying a mask generation function (MGF) to the second random number and converting it into a string with the same length as the first random number, via step 414. MGF's are well known in the art. The first random number and the third random number are XOR'ed to generate a fourth random number, via step 416. This fourth random number is stored, via step 418. The migratable keyblob 202 is migrated from the computer with the TPM to itself, via step 420.

To use the parent key 108, the user enters his/her pass phrase. Figure 5 is a flowchart illustrating how a key secured with the method in accordance with the present invention is obtained. First, the user's pass phrase is received, via step 502. The third random number is then obtained from hashing the pass phrase and applying the MGF, via step 504. The first

random number is then obtained by XOR'ing the third random number with the stored fourth random number, via step 506. The TPM's random number and the encrypted migratable keyblob 202 are then sent to the TPM 102, via step 508. The TPM 102 unwraps the encrypted migratable keyblob 202 using its private key, via step 510. The TPM 102 XOR's the migratable keyblob 202 with the first random number to obtain the scrambled parent key 108, via step 512. The TPM 102 can then unscramble the parent key 108, via step 514. Once unscrambled, the key 108 may be used. While with a conventional migratable keyblob, the recovered key 10 is rewrapped into a normal blob and stored in persistent memory, this does not happen with the recovered key 108 in accordance with the present invention. The returned normal blob is discarded instead.

Alternatively, if the security provided by the migratable keyblob is not required, then a non-migratable keyblob can be used. A random number of equal length to the non-migratable keyblob can be provided by the TPM 102 and XOR'ed with the non-migratable keyblob. The results is stored. The random number is then hidden by encrypting it with a key derived from the user's pass phrase.

A method for providing improved security with a secure chip has been disclosed. The method stores a key in the secure chip's key chain within a migratable keyblob. The random number used to create the migratable keyblob is stored encrypted using a pass phrase of a user of the key. If the root key of the secure chip is somehow stolen, the thief can only unwrap keys in the key chain which are ancestors of the key stored in the migratable keyblob. To obtain the key in the migratable keyblob, the random number used to create it is required. However, the pass phrase of the user is required to decrypt it. This increases the security of the key stored in the migratable keyblob and its children keys.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.